

### **Remarks**

The Applicant respectfully requests reconsideration and reexamination of the above-identified patent application, with amendment. Claims 1-9 are pending in this application upon entry of this Amendment. In this Amendment, the Applicant has amended claims 1, 3, 5, and 8. No claims have been cancelled or added in this Amendment. Of the pending claims, claims 1, 3, 5, and 8 are independent claims.

### **Claim Rejections – 35 U.S.C. § 102**

In the Office Action mailed June 29, 2006, the Examiner rejected claims 1-9 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,556,681 issued to King (“King”). The Applicant respectfully traverses and has amended independent claims 1, 3, 5, and 8 to more clearly set forth the claimed subject matter.

For purposes of describing patentable differences between the claimed subject matter set forth in the amended independent claims presented herein and King, the Applicant provides the following comparison between amended independent claim 1 and King.

#### **1. Amended Independent Claim 1**

Amended independent claim 1 recites a keyless authorized access control system. The system includes at least two object modules (“OMs”) and at least one identification (“ID”) device. Each OM is assigned to a respective object. Each ID device has a microprocessor and a memory element.

Each ID device and the OMs have respective bidirectional data communications links between them for communicating encoded data. The data communicated between an ID device and each OM is encoded by an encryption algorithm and a symmetric encryption method which uses an encryption parameter. Encryption algorithms and encryption parameters are uniquely assigned to the OMs.

The memory element of each ID device stores at least two different encryption algorithms and at least two different encryption parameters including the encryption algorithms and the encryption parameters assigned to the OMs. The microprocessor of an ID device selects from the stored encryption algorithms and encryption parameters the encryption algorithm and the encryption parameter assigned to an OM to be used with the symmetric encryption method for encoding the data to be communicated between the ID the OM.

**2. Amended Independent Claim 1 Compared to King**

Amended independent claim 1 differs from King in that the ID device stores at least two different encryption algorithms and at least two different encryption parameters including encryption algorithms and encryption parameters uniquely assigned to the OMs, the ID device selects from the stored encryption algorithms and encryption parameters the encryption algorithm and the encryption parameter assigned to an OM to be used with a symmetric encryption method for encoding the data to be communicated between the ID device and the OM such that the data communicated between the ID device and the OM is encoded by the selected encryption algorithm and the symmetric encryption method which uses the selected encryption parameter.

In contrast, King describes data modules for a trainable transmitter in which the data modules are assigned to respective objects and respectively include data necessary to generate codes for the respective objects. The data for generating a code for an object may include a cryptographic algorithm. King describes a cryptographic algorithm is one used for generating a rolling code but is not used for generating a fixed code (see col. 2, lines 29-41 of King). In the case of a fixed code, the code is not “encrypted” (see col. 2, lines 38-41 of King). As such, a cryptographic algorithm described by King is an algorithm used to generate a code and is similar in function to the claimed symmetric encoding method which uses an encryption parameter to generate data. However, King does not teach or suggest an encryption algorithm as claimed which would be further used to encrypt a generated rolling code (which has been generated using a cryptographic algorithm as described by King) or a fixed code (which has been generated without the use of a cryptographic algorithm as described by King).

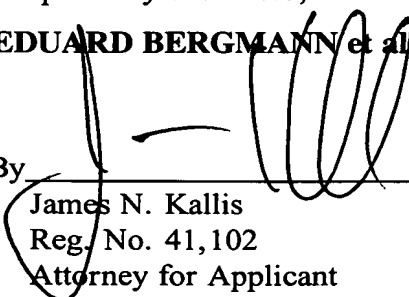
As claimed, each object module is uniquely assigned an encryption parameter used with a symmetric encryption method for encrypting data to be communicated between the object module and an ID device and is further uniquely assigned an encryption algorithm which is used further used to encrypt the data to be communicated between the object module and the ID device. As described, King does not teach or suggest this latter element.

In view of the foregoing amendments and remarks, the Applicant respectfully submits amended independent claims 1, 3, 5, and 8 are patentable over King. Claims 2, 4, 6-7, and 9 depend from one of the amended independent claims and include the limitations of their respective independent claim. Accordingly, the Applicant respectfully requests reconsideration and withdrawal of the 35 U.S.C. § 102(e) rejections of claims 1-9.

### CONCLUSION

In summary, claims 1-9 presented herein meet the substantive requirements for patentability. The case is in appropriate condition for allowance. The case is in appropriate condition for allowance. If a telephone or video conference would expedite allowance or resolve any further questions, such a conference is invited at the convenience of the Examiner.

Respectfully submitted,  
**EDUARD BERGMANN et al.**

By   
James N. Kallis  
Reg. No. 41,102  
Attorney for Applicant

Date: October 30, 2006

**BROOKS KUSHMAN P.C.**  
1000 Town Center, 22nd Floor  
Southfield, MI 48075-1238  
Phone: 248-358-4400  
Fax: 248-358-3351